UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IQVIA INC. and IMS SOFTWARE SERVICES, LTD., *Plaintiffs – Counterclaim Defendants,* v. VEEVA SYSTEMS INC., *Defendant – Counterclaim Plaintiff.*	Case No.: No. 2:17-cv-00177-CCC-MF Hon. Claire C. Cecchi Hon. Mark Falk, U.S.M.J. Hon. Dennis M. Cavanaugh, Ret. U.S.D.J. [redacted] Motion Return Date: July 6, 2021 *Document Filed Electronically* **ORAL ARGUMENT REQUESTED**

VEEVA SYSTEMS INC.'S BRIEF IN SUPPORT OF ITS OBJECTIONS TO [DKT. 349] THE SPECIAL DISCOVERY MASTER's ORDER OF MAY 7, 2021, RECOMMENDING SANCTIONS

Joseph A. Hayden
David N. Cinotti
PASHMAN STEIN WALDER HAYDEN, P.C.
Court Plaza South
21 Main Street, Suite 200
Hackensack, NJ 07601
Tel: (201) 488-8200
jhayden@pashmanstein.com
dcinotti@pashmanstein.com

Steven F. Benz
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
Tel: (202) 326-7900
sbenz@kellogghansen.com

James T. Southwick
SUSMAN GODFREY L.L.P.
1000 Louisiana, Suite 5100
Houston, TX 77002
Tel: (713) 651-9366
jsouthwick@susmangodfrey.com

Charles T. Graves
WILSON SONSINI GOODRICH & ROSATI PC
One Market Plaza, Spear Tower, Suite 3300
San Francisco, CA 94105
Tel: (415) 947-2000
Tgraves@wsgr.com

Counsel for Defendant/Counterclaim-Plaintiff Veeva Systems Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

INTRODUCTION

The Special Master found that Veeva spoliated records and recommended that, if IQVIA proves spoliation at trial, then this Court should instruct the jury that it may infer that the deleted records would have advanced IQVIA's trade-secret misappropriation claims. The Special Master's findings and recommendations have no basis in fact or law. Adverse-inference sanctions require bad intent. Veeva has acted in good faith, and its discovery efforts have exceeded its obligations.

Veeva acknowledges the gravity of the questions presented. Veeva is a public-benefit corporation that places the utmost value on honesty, fairness, and candor. Indeed, the goal of Veeva's antitrust claim is to make the life sciences industry fairer, more transparent, and more conducive to innovation. Destroying documents to gain a litigation edge is antithetical to Veeva's most hallowed precepts. The Special Master's order was shocking and dispiriting to the individuals within Veeva who have worked tirelessly to uphold Veeva's values in this lawsuit—individuals whose efforts were mischaracterized by IQVIA and misunderstood by the Special Master.

The truth is that Veeva's discovery efforts have been laudable. When IQVIA filed its lawsuit, Veeva worked to freeze vast document repositories covering thousands of current and former employees globally. Veeva rendered deletion of email and other communications a technical impossibility. Veeva produced millions of documents and gave its direct competitor full working copies of its proprietary software and data products—the very products into which IQVIA claims its trade secrets were incorporated. Contrary to the Special Master's ruling, there is no basis to conclude that Veeva intentionally destroyed evidence while anticipating litigation. Clearly established law and unrebutted evidence require reversal of four points of error:

First, the Special Master held that Veeva's duty to preserve arose 16 months before IQVIA filed this lawsuit and [redacted] before IQVIA started preserving its own documents. That finding

is unprecedented. In September 2015, Veeva discovered a technical error (the "Genentech incident") in one of its software systems. Veeva initially feared that IQVIA's proprietary data leaked into Veeva's data product. Veeva's investigation dispelled that concern and confirmed that the incident affected only a tiny sliver of public data that Veeva already obtained from other sources. Since the incident proved inconsequential, it could not have triggered a duty to preserve.

Second, the Special Master found that the scope of Veeva's preservation duty was near-limitless. That too was error. A party need only preserve relevant documents. Even if the Genentech incident triggered a preservation duty (it did not), that duty could not apply to *unrelated* documents. Yet the Special Master found that Veeva's duty extended not only to Genentech-related materials but also to mountains of unrelated records. The Special Master's approach would require corporations to engage in sweeping, expensive, and wasteful preservation efforts that neither the Federal Rules nor governing caselaw require.

Third, the Special Master found that Veeva spoliated a defunct software environment called EUStage. Yet the record does not suggest bad faith, and the EUStage data still exists. Veeva mistakenly swept EUStage into its policy of deleting *all* inactive software environments as it transitioned to the Amazon Web Services ("AWS") infrastructure. Although Veeva deleted the EUStage *software environment*, Veeva archived all EUStage *data*, which remains available.

Fourth, the Special Master held that Veeva spoliated custodian James Kahan's January 2014–May 2015 emails. But Kahan's emails were deleted pre-litigation, before Veeva had a duty to preserve. Veeva presented unrebutted evidence that Kahan's emails were deleted to free up space in his email inbox—not to destroy evidence. Veeva produced 6,800 of Kahan's January 2014–May 2015 emails and 65,000 of Kahan's emails from outside that period, confirming Veeva's good faith. IQVIA failed to show that any relevant emails were deleted.

BACKGROUND

In life sciences technology markets, data and software are interdependent—one cannot function without the other. IQVIA has monopolized the life sciences data markets for decades.[1] But it has struggled to parlay its data dominance into software success.[2] Meanwhile, Veeva has become the life sciences industry's most innovative software company. In 2007, Veeva introduced its Customer Relationship Management ("CRM") application, marking the industry's transition to cloud-based commercial software.[3] Six years later, Veeva unveiled Veeva Network, master data management ("MDM") software that generates up-to-date healthcare information.[4] To complement its software, Veeva launched its own reference data[5] product called OpenData.[6]

Veeva's growth roiled IQVIA. By devising cutting-edge commercial software tailored to life sciences, Veeva had accomplished what IQVIA could not. Worse, OpenData's advent jeopardized IQVIA's monopolies. To prevent customers from adopting Veeva Network and leaving it in the dust, IQVIA hatched a plan. IQVIA knew that Veeva Network was useless without reference data, and that IQVIA's OneKey was the entrenched reference data product. So IQVIA refused to sign Third-Party Access ("TPA") agreements permitting customers to use OneKey in Network. Starved of data, Veeva's new software product would wither.

IQVIA grasped the power of its machinations. It understood that reference data [redacted] IQVIA knew that this

[1] *E.g.*, Ex. 1 at 766; Ex. 2 at 313.
[2] Ex. 3 at 166:23–24; Ex. 4 at 115:25–116:1; Ex. 5 at 379.
[3] Ex. 6 at 278.
[4] *See* Ex. 7 at 22:3–12.
[5] "Reference data" refers to information on healthcare professionals and healthcare organizations.
[6] Ex. 8 at 665–66.
[7] Ex. 9 at 083.

[redacted] would have substantial [redacted]

By design, IQVIA's TPA policy harmed customers. IQVIA observed that what [redacted] was IQVIA's refusal to lets its [redacted] which [redacted][9] [redacted] lamented, [redacted][10] To placate customers, IQVIA masqueraded its TPA policy as an IP safeguard. Yet IQVIA could never articulate precisely *how* Veeva "endangered" IQVIA's IP. As [redacted] noted, [redacted]

Although IQVIA's IP concerns were manufactured, Veeva worked ceaselessly to address them. Veeva gave IQVIA detailed assurances of Network's protections,[12] and IQVIA acknowledged their effectiveness.[13] When IQVIA's groundless concerns persisted, Veeva agreed to submit Network to an [redacted] audit by [redacted]. [redacted][14]

[8] *Id.* (all emphasis added unless otherwise noted); *see also* Ex. 10 at 506.
[9] Ex. 11 at 315.
[10] Ex. 12 at 364.
[11] Ex. 13 at 154:8–155:16.
[12] *E.g.*, Ex. 14 at 258; Ex. 15 at 108.
[13] Ex. 16 at 273 [redacted].
[14] Ex. 17 at 327.

In September 2015, Veeva prepared for the audit by launching an internal investigation. That investigation uncovered an unrelated access-configuration error (the "Genentech incident"). The error was not in Veeva Network—the focus of this lawsuit—but rather in a separate Veeva system called Healthcare Data Management ("HDM"), which Veeva used for customer-specific data-services projects.[15] A company that Veeva acquired years earlier called AdvantageMS ("AMS") was responsible.[16] The error caused certain IQVIA records provided to Veeva by customer Genentech (with IQVIA's permission) to be inadvertently included as contribution sources for Veeva OpenData's address validation process.[17] Those records were potentially viewable by certain Veeva personnel.[18]

Veeva investigated and established four key findings:

- First, the scope of the error was microscopic, implicating only 1,350 IQVIA records—***0.00063%*** of the OpenData dataset.[19]
- Second, the error was inconsequential, affecting only ***publicly available addresses*** that Veeva had ***already obtained*** from other sources.[20]
- Third, the error was ***fully remediable***, as Veeva "removed immediately" all IQVIA data from OpenData and installed strict controls to prevent similar incidents.[21]
- Fourth, there was ***no evidence*** that Veeva employees ever accessed the impacted records to improve OpenData, or that employees even knew they had such access before Veeva's remediation eliminated it.[22]

---

[15] Ex. 18 at 764.
[16] Ex. 19 at 002, 004.
[17] *Id.* at 002.
[18] *Id*. at 003.
[19] Ex. 18 at 763 (calculated by dividing (i) the product of the 1,350 IQVIA addresses and five IQVIA address fields, by (ii) the product of 10,886,231 OpenData addresses and 98 OpenData address fields).
[20] *Id*. at 764.
[21] Ex. 19 at 004–005.
[22] Ex. 20. ¶ 18; *see also* Ex. 21 at 78:9–25 (Veeva's OpenData stewards did not [redacted]

After confirming that the incident was a nonissue unrelated to the EY audit (which focused on Veeva Network, *not* the HDM system in which the incident occurred), Veeva proceeded with the audit. EY detected no material issues and Veeva cured all minor ones.[23]

In April 2016, customer Shire expressed interest in a data report card ("DRC"). DRCs are industry-standard tools by which data vendors demonstrate their products' accuracy by comparing them to prospective customers' incumbent datasets.[24] Before obtaining the customer-data extracts on which to perform DRCs, Veeva required customers to affirm their right to transfer the extracts to Veeva.[25] Shire provided such affirmation, so Veeva proceeded.[26] Shire later determined that, contrary to its prior representation, it was not entitled to convey the extract to Veeva because it contained IQVIA data for which IQVIA had not issued a TPA.[27]

Veeva investigated the Shire incident and told IQVIA that the Shire extract "has been deleted and did not contribute to Veeva's OpenData product."[28] Veeva explained, "We do not retain any extracted data used to create data reports [i.e., DRCs]. If any IMS data was sent to Veeva in the past in similar circumstances, it does not persist at Veeva and did not contribute to Veeva OpenData."[29] IQVIA responded, [redacted]

[23] Ex. 22 at 809 [redacted]
Ex. 23 at 302.
[24] *See, e.g.*, Exs. 24–28.
[25] *E.g.*, Ex. 29 at 070; Ex. 30.
[26] *E.g.*, Ex. 31 at 010–12.
[27] Ex. 32 at 013.
[28] Ex. 33 at 779.
[29] *Id*. at 777.
[30] *Id*. at 776.

The parties' TPA negotiations resumed. Although it is now clear that IQVIA never intended to resolve the impasse, IQVIA had lured Veeva toward the belief that resolution was imminent. [redacted].[31] Unable to support its "IP concerns," yet unwilling to budge on TPA policy, IQVIA sued Veeva and has used this lawsuit to justify its monopolistic behavior to customers.

In February 2020, IQVIA moved for sanctions against Veeva, alleging that Veeva's discovery of the Genentech incident triggered its preservation duty. IQVIA claimed Veeva breached that duty by deleting (1) customer-data files contained in HDM and a related storage server called "Network Attached Storage" ("NAS"); (2) communications relating to the Shire incident; (3) EUStage; (4) Kahan's January 2014–May 2015 emails; and (5) Google-Drive documents. Dkt. 284. The Special Master recommended adverse-inference sanctions and awarded costs and fees as to categories (1), (3), and (4), and declined to sanction Veeva with respect to (2) and (5). Dkt. 349.

LEGAL STANDARD

The district court "must decide de novo all objections to conclusions of law" and "findings of fact made or recommended by" the Special Master. Fed. R. Civ. P. 53(f)(3)–(4). A court may impose an adverse-inference sanction only where a party loses or deletes relevant evidence it was obligated to preserve, with intent to deprive the opposing party of that evidence. Fed. R. Civ. P. 37(e)(2). A court may impose monetary sanctions where a party negligently loses or deletes relevant evidence it was obligated to preserve. Fed. R. Civ. P. 37(e)(1).

[31] Ex. 34 at 735; Ex. 35 at 65:2–12.

ARGUMENT

I. Error No. 1: The Special Master wrongly held that Veeva's duty to preserve arose 16 months before IQVIA sued and [redacted] before IQVIA began preserving documents.

The Special Master erroneously found that Veeva should have anticipated litigation when it discovered the Genentech incident in September 2015, commencing its duty to preserve. Dkt. 349 at 70. IQVIA did not sue, threaten to sue, or hint at litigation in 2015. The Special Master held that, even in the absence of a lawsuit or demand letter, a few nonlawyer-employees' vague concerns about potential litigation created a broad and indefinite duty to preserve. IQVIA cited no authority for that principle. None exists.

"Before sanctions for spoliation can be imposed, it must be determined whether the duty to preserve evidence has been triggered." *Kounelis v. Sherrer*, 529 F. Supp. 2d 503, 518 (D.N.J. 2008). The duty arises "when the party in possession of the evidence knows that litigation by the party seeking the evidence is ***pending or probable***." *State Nat'l Ins. Co. v. Cty. of Camden*, 2011 WL 13257149, at *2 (D.N.J. June 30, 2011). Sensibly, the law does not require litigants to preserve documents on the off-chance that litigation might arise. To the contrary, courts have cautioned against imposing onerous obligations that would require companies to expend vast resources hoarding useless information. That is why courts have established clear rules.

The duty to preserve typically does not activate until "suit has already been filed." *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). Occasionally, a pre-lawsuit "[demand] letter, … request for evidence preservation, [or] threat of litigation" may trigger the duty. *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 327 F.R.D. 96, 106 (E.D. Va. 2018). But neither a "general concern over litigation" nor the "mere existence of a dispute" suffices. *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 264 F.R.D. 517, 524 (N.D. Cal. 2009); *Goodman v. Praxair Servs., Inc.*, 632 F. Supp. 2d 494, 510 (D. Md. 2009). The facts in *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244

F.R.D. 614 (D. Colo. 2007), illustrate the rarity of pre-litigation preservation duties. Cache sent a letter asserting its trademark rights and warning Land O'Lakes to "avoid exposure" and "litigation." *Id*. at 622–23. The letter did not trigger a preservation duty because it was too "equivocal" in "threaten[ing] litigation." *Id*. at 623.

The Genentech incident was insufficiently severe to activate the extraordinary pre-litigation preservation duty. The incident proved minor, rendering litigation unforeseeable.

A. Veeva's internal investigation established that the Genentech incident was small, practically inconsequential, and unlikely to lead to litigation.

Veeva discovered the Genentech incident in connection with an internal investigation that, while spawning some panicked internal communications, culminated in a finding that litigation was unlikely. The law does not impose a preservation duty under those circumstances.

When a party investigates a potential incident and reasonably concludes it was a minor mishap, litigation is not "probable" and no duty to preserve arises. In *United States v. Kitsap Physicians Service*, 314 F.3d 995 (9th Cir. 2002), Kitsap investigated potential fraud among its employees, found that no fraud occurred, and destroyed related billing records pursuant to document retention policies. *Id*. at 998–99. Plaintiff claimed that the fraud inquiry triggered Kitsap's duty to preserve. *Id*. at 1001. The court disagreed, explaining that "the result of this investigation was an opinion from outside legal counsel that there were no bases for fraud. From the defendants' perspective, they were not on notice of potential litigation, much less a specific, future *qui tam* lawsuit." *Id*. Plaintiff's untenable position would have required corporations to "keep documents in perpetuity where there was a single suggestion of possible" wrongdoing even if that possibility was discredited. *Id*.

Putscher v. Smith's Food & Drug Centers, Inc., 2014 WL 2835315 (D. Nev. June 20, 2014), stands for the same principle: corporate knowledge of a potential violation, even coupled

with concern about prospective litigation, does not trigger the preservation duty unless litigation was objectively "probable." There, Smith's investigated plaintiff's fall in its store and concluded that the incident was minor. *Id*. at *1–2. The court agreed, holding that Smith's had no duty to preserve surveillance footage of the fall even though Smith's had prepared an incident report that read, "This report is being prepared in anticipation of litigation under the direction of legal counsel." *Id*. Despite that language, no duty arose because Smith's reasonably concluded that plaintiff's fall was nonserious and that litigation was not likely. *Id*.

Likewise, in *Sudre v. The Port of Seattle*, 2016 WL 7035062 (W.D. Wash. Dec. 2, 2016), after plaintiff fell in the defendant Port's airport, the Port investigated, found that it was not at fault, and deleted footage of the accident under its retention policies. *Id*. at *1, 24–25. Although it prepared a "general liability report," the Port was not obligated to preserve the footage because it reasonably concluded that plaintiff's fall was trivial, rendering litigation improbable. *Id*.

Kitsap, *Putscher*, and *Sudre* demonstrate that litigation was not "probable" in light of the Genentech incident. Veeva's investigation uncovered no misappropriation. Rather, Veeva established that the incident was minute, affecting ***0.00063%*** of the OpenData dataset.[32] Veeva confirmed that the incident implicated only ***publicly available addresses*** that Veeva had ***already obtained*** from State Medical Boards, the Center for Medicare and Medicaid Services, and the Drug Enforcement Administration.[33] Veeva unearthed ***no evidence*** that employees accessed, or knew they could access, the affected addresses.[34] Veeva ***fully remediated*** the incident and ensured it

[32] Ex. 18 at 763.
[33] *Id*. at 764; *see also* Ex. 36 at 105 [redacted]
[34] Ex. 20 ¶ 18; Ex. 19 at 001 [redacted] Ex. 21 at 78:9–25.

could not repeat.[35] Veeva's findings were unequivocal: Founder and CEO Peter Gassner concluded that the incident was a "minor," "small thing" affecting only "non sensitive data that was publicly available."[36] Veeva's General Counsel did not "anticipate potential litigation against IMS" because the incident implicated "a very minor, limited amount of records involving addresses."[37] As in *Kitsap*, *Putscher*, and *Sudre*, Veeva investigated and found no basis for litigation (much less the specific trade-secret lawsuit IQVIA filed 16 months later), foreclosing any duty to preserve.

Veeva was correct in concluding that litigation was improbable. First, independent derivation of alleged trade secrets forecloses misappropriation. 18 U.S.C. § 1839(6)(B). Veeva independently derived all 1,350 affected addresses from other sources.[38] Second, to constitute a "trade secret," information must "not be[] readily ascertainable through proper means." *Id.* § 1839(3)(B). Beyond "readily ascertainable," all 1,350 affected addresses were *publicly available*[39] and cannot qualify as "trade secrets."[40] Third, misappropriation requires acquiring or disclosing information *with knowledge* that the information is a trade secret and that the trade secret was improperly obtained. *Id.* § 1839(5); N.J. Stat. Ann. § 56:15-2. IQVIA authorized Veeva

[35] Ex. 19 at 004–005.
[36] Ex. 36 at 103–04.
[37] Ex. 38 at 120:20–121:9.
[38] Ex. 18 at 764 [redacted]
[39] *Id*; Ex. 39 at 826 [redacted] *see also* NPPES NPI Registry, *Search NPI Records*, https:npiregistry.cms.hhs.gov/registry/? (doctor and hospital addresses publicly available on command).
[40] *E.g.*, *Baxter Healthcare Corp. v. HQ Specialty Pharma Corp.*, 157 F. Supp. 3d 407, 424 n.48 (D.N.J. 2016) (finding Baxter's trade secret claims "unsupportable" because they derived from "publicly available" information); *Vital State Canada, Ltd. v. DreamPak, LLC*, 202 F. Supp. 2d 516, 527 (D.N.J. 2003) (rejecting "claimed trade secrets" that "were or are now all generally known to the public"); *SI Handling Sys., Inc. v. Heisley*, 753 F.2d 1244, 1255–56 (3d Cir. 1985) (courts must consider whether "the information is known outside of the owner's business" in assessing whether it is "a trade secret").

to obtain the 1,350 addresses from Genentech and perform services on Genentech's behalf. Veeva could not have known that a configuration error in a system acquired from AMS would cause the 1,350 addresses to validate records in OpenData.[41] Veeva remedied the error immediately upon discovering it.[42] Even if the 1,350 addresses constituted "trade secrets," Veeva never acquired or disclosed them with the knowledge that they were improperly obtained, precluding misappropriation. Fourth, IQVIA's own conduct confirms the incident's mildness. [redacted]

The incident did not alert Veeva to probable litigation, much less a specific misappropriation lawsuit. *See Kitsap*, 314 F.3d at 1001. A contrary ruling would cripple businesses nationwide by compelling them to "keep documents in perpetuity where there was a single suggestion of possible" impropriety even where that possibility was probed and debunked. *See id.*

B. The Data Corruption Memo confirms that litigation was not "probable" following the Genentech incident.

The Special Master relied on the "Data Corruption Memo"[44] in concluding that the Genentech incident triggered Veeva's duty to preserve. Dkt. 349 at 71. The Special Master found that the Memo "contemplates that IQVIA will file a lawsuit as a result of the Genentech Incident and that Veeva's exposure could be high." *Id*. Yet the Memo confirmed that the incident implicated

[41] Ex. 39 at 833 [redacted]

[42] *Id*. at 827–28.

[43] Ex. 41 (Veeva's Apr. 27, 2018 Responses to IQVIA Irogs.) at 15; Ex. 44 [redacted].

[44] Ex. 39.

an undetectable trace of public information that Veeva had already obtained elsewhere,[45] rendering litigation unlikely. That is why the Memo identified litigation as only a "***Potential Risk***."[46]

A "potential risk" of litigation cannot trigger the duty to preserve. *E.g.*, *Kounelis*, 529 F. Supp. 2d at 518 (litigation must be "***pending or probable***" to trigger duty to preserve); *Hynix Semiconductor v. Rambus*, 591 F. Supp. 2d 1038, 1061 (N.D. Cal. 2006) (litigation must be "***more than a possibility***" to require preservation); *Turner v. Hudson Transit lines*, 142 F.R.D. 68, 73 (S.D.N.Y. 1991) (duty to preserve arises when litigation is "***likely to be commenced***"); *Cache*, 244 F.R.D. at 621 ("[D]uty to preserve relevant documents should require ***more than a mere possibility*** of litigation."); *Goodman*, 632 F. Supp. 2d at 510 (a "***general concern*** over litigation" does not trigger duty to preserve); *Winn-Dixie Stores v. Dollar Tree Stores*, 2012 WL 12877648, at *1 (S.D. Fla. Mar. 12, 2012) ("duty to preserve" requires more than a "***mere possibility***"). The Special Master himself noted that the Memo merely "***contemplates***" litigation—and contemplation alone cannot trigger a preservation duty. Dkt. 349 at 71.

No court has imposed a preservation duty based on a "potential risk" of litigation. In *Putscher*, 2014 WL 2835315 at *1–2, defendant's incident report explicitly "prepared in anticipation of litigation" did not trigger the duty because defendant concluded that plaintiff's fall was mild. In *Sudre*, 2016 WL 7036062 at *24–25, defendant's "general liability report" did not activate its duty because it found plaintiff's accident was benign. And in *Rocker Management v. Lernout & Hauspie Speech Products*, 2007 WL 9782803 (D.N.J. July 12, 2007), no preservation duty arose even though defendant Cowen assumed it would be targeted by litigation. After

[45] *Id*. at 825–27, 832 [redacted]

[46] *Id*. at 831; *see also id*. at 825.

Cowen's conspirator fell under SEC investigation, a Cowen witness "testified that Cowen employees openly discussed the fact that the company would be sued" and he "assumed there would be lawsuits surrounding the SEC investigation." *Id*. at *10. This Court held that Cowen's duty had not commenced because the witness "testified very generally" that "Cowen would be sued when the investigation began" but "did not testify that the September 21, 2000 SEC investigation would *likely* result in litigation." *Id*. Since *Putcher*'s "anticipation of litigation," *Sudre*'s "general liability report," and *Rocker*'s "assum[ption] there would be lawsuits" did not trigger a preservation duty, Veeva's identification of "Potential Risks" plainly fell short. Indeed, the Memo's author testified that he was asked to "brainstorm the worst-case scenarios that might emerge from the Genentech data issues," including all "conceivable risks," "however remote."[47]

The Special Master further erred in finding that the Memo "contemplate[d]" that "Veeva's exposure could be high." Dkt. 349 at 71. Where the Memo considered possible "Financial Damage" up to "10M" and the "Potential for other damages," it referred to conjectural "*Financial* Risk" such as lost business opportunities or disrupted contracts.[48] Those portions of the Memo did not refer to *legal* risk.[49] Potential commercial losses untethered to litigation cannot trigger the duty to preserve. *See State Nat'l Ins. Co.*, 2011 WL 13257149, at *2.

C. Veeva nonlawyers' uninformed statements do not support "probable" litigation following the Genentech incident.

The Special Master relied on the paranoid remarks of Veeva nonlawyer-employees Rebecca Silver and Brian Longo in concluding that the Genentech incident triggered Veeva's preservation duty. Dkt. 349 at 71. Yet courts discount the importance of nonlawyer statements in

[47] Ex. 37 ¶¶ 7–8.
[48] *Id*.
[49] *Id*.

assessing the duty to preserve, as nonlawyers lack litigation-hold experience. For instance, in *Rocker*, 2007 WL 9782803 at *10, an SEC probe did not trigger Cowen's preservation duty despite Cowen-employee testimony "that he assumed there would be lawsuits surrounding the SEC investigation." This Court explained that the testimony was "not significant" since the witness "was not deposed as an expert on litigation holds" and "was not a member of Cowen's legal department and, therefore, likely had no authority to implement a litigation hold." *Id*.

By the same token, Silver and Longo are data and software specialists—not litigation-hold experts and not members of Veeva's legal department. They did not, and were not competent to, testify to Veeva's expectation of litigation. Meanwhile, Veeva's General Counsel Josh Faddis instituted Veeva's litigation hold and testified that Veeva did not "anticipate potential litigation against IMS" because the Genentech incident affected a "very minor, limited amount of records involving addresses" and was "unlikely to have led to litigation."[50] The Special Master erred in relying on nonlawyer statements while ignoring Veeva's counsel's.

Moreover, Silver and Longo made those statements mid-investigation, before ascertaining the incident's scope. When Veeva uncovered the Genentech incident on September 21, 2015, the facts were unclear.[51] Silver and Longo uttered the statements on September 21 and 22, as uncertainty persisted.[52] It was not until September 24–25 that Veeva began to grasp the incident's scope.[53] Once it did so, Veeva recognized that the incident was a "minor thing" implicating a "small amount" of "non sensitive data that was publicly available."[54] The Special Master erred in

[50] Ex. 38 at 120:20–121:9; *see also* Ex. 20. ¶¶ 18–19.
[51] Ex. 39 at 825 [redacted] Ex. 20 ¶ 18.
[52] Ex. 42 at 619–20; Ex. 43 at 010–11.
[53] Ex. 19. Even then, Veeva continued working to confirm the incident's scope. *Id*. at 004.
[54] Ex. 36 at 103–04.

relying on uninformed statements while disregarding executive-level legal conclusions reached in light of the investigation's findings. Dkt. 349 at 71.

D. Events after September 2015 confirm that litigation was not "probable" until IQVIA sued Veeva in January 2017.

The Genentech incident was a technical error by which Veeva inadvertently accessed IQVIA data without a TPA. Seven months later, customer Shire's oversight led to the same result.[55] When Veeva discovered the issue, it cured the harm by purging the IQVIA data. After learning about Veeva's access to and deletion of IQVIA data, IQVIA did not sue, threaten to sue, or even hint at litigation. Instead, [redacted][56]

The Shire incident proves that a small-scale data-access issue would not have provoked litigation. [redacted] Since an insufficiently clear demand letter does not trigger the preservation duty, [redacted] fell short. *Cache*, 244 F.R.D. at 623; *Turner v. United States*, 736 F.3d 274, 282 (4th Cir. 2013) ("[P]laintiff ...did nothing to trigger a duty to preserve" as "[s]he did not send ...a document preservation letter, or any other correspondence threatening litigation."). The improbability of litigation following the Shire incident proves that IQVIA would not have sued after the similar Genentech incident. *See Bistrian v. Levi*, 448 F. Supp. 3d 454, 468 (E.D. Pa. 2020) (looking to the "course of conduct between the parties" in assessing the preservation duty).

[55] *See supra* at 6–7.
[56] Ex. 33 at 776.
[57] Ex. 45 [redacted]; Ex. 46 at 32:19–33:1 [redacted].

The Special Master found that comparing the Shire and Genentech incidents was "improper," reasoning that "had IQVIA been aware of the Genentech Incident, it may have reacted very differently to the Shire Incident." Dkt. 349 at 72. But the question is how IQVIA would have reacted to the *Genentech incident* (the purported duty-triggering event), not to the *Shire incident*. IQVIA claims [redacted].[58] The Shire incident disproved that assertion. Had IQVIA been aware of the Genentech incident, it would have reacted as it did to the Shire incident—not with litigation or threatened litigation, but with [redacted]. *See MacNeil Auto. Prods. v. Cannon Auto.*, 715 F. Supp. 2d 786, 801 (N.D. Ill. 2010) (no preservation duty where "Defendant had supplied defective mats to Plaintiff on occasions prior … but legal proceedings never resulted—the parties were able to resolve the dispute among themselves" and "continued their business relationship"); *Philmar Dairy v. Armstrong Farms*, 2019 WL 3037875, at *3–5 (D.N.M. July 11, 2019) (no duty in part because "the parties had done business for years 'without incident'").

The Special Master wrongly distinguished the Shire incident from the Genentech incident by pointing out Veeva's nondisclosure of the latter during the EY audit. Dkt. 349 at 72. But Veeva did not disclose the incident for a simple reason: it had no duty or reason to do so. The incident was outside the audit's scope, which addressed Veeva Network—*not* HDM (the source of the Genentech incident). [redacted] Veeva truthfully answered [redacted] IQVIA's general counsel and orchestrator of the EY audit acknowledged

[58] Ex. 47 at 6.
[59] Ex. 48 at 344, 346 [redacted]; *id.* [redacted]

that the [redacted][60]

To be sure, the Corruption Memo contemplated that the audit might encompass the Genentech incident.[61] When the Memo was written, "the scope of the audit was in flux and had not been finalized."[62] To ensure its preparedness, Veeva planned as though the audit would sweep broadly.[63] The parties then confirmed that the audit would cover only Veeva Network—the subject of the parties' TPA dispute.[64] Since the Genentech incident arose from HDM, not Veeva Network, "the Genentech data issues exceeded the EY audit's scope."[65]

Finally, the Special Master observed that "after the Shire Incident, Veeva made assurances to IQVIA that the data was promptly deleted, and was not retained, used or viewable by any Veeva personnel. Veeva cannot say the same for the Genentech Incident." Dkt. 349 at 72. But Veeva *can* say the same for the Genentech incident. After the incident, Veeva removed the corrupted IQVIA records from OpenData.[66] Veeva found "no proof that the customer and 3rd party data was used to improve OpenData."[67] And in both instances, IQVIA data was potentially accessible to Veeva personnel, but Veeva never attempted to exploit that access to improve OpenData. In light of [redacted], the Special Master erred in finding that Veeva should have expected litigation following the Genentech incident.

---

[60] Ex. 49 at 059; Ex. 50 at 217 [redacted]
[61] Ex. 39 at 826.
[62] Ex. 37 ¶ 10.
[63] *Id*.
[64] *Id*. ¶ 11.
[65] *Id*.
[66] Ex. 39 at 826–28.
[67] *Id*. at 832.

The Genentech incident did not trigger Veeva's pre-litigation duty to preserve. Since any deletions of NAS directories, HDM tables, and Kahan emails occurred pre-litigation, they cannot support adverse-inference or monetary sanctions. Fed. R. Civ. P. 37(e).

II. Error No. 2: The scope of any duty to preserve arising from the Genentech incident could not have extended to irrelevant NAS directories and HDM tables.

Even if the Genentech incident had triggered Veeva's preservation duty, the Special Master misstated the duty's *scope*. The Special Master extended Veeva's duty to "200 NAS directories and thousands of tables and databases deleted from HDM." Dkt. 349 at 73. "NAS," short for "Network Attached Storage," is a server where Veeva stored data files received from customers, called "NAS directories." "HDM tables" refers to customer data that Veeva loaded onto HDM to perform services for those customers. The NAS directories and HDM tables cited in IQVIA's motion bore no connection to the Genentech incident. The incident could not have obligated Veeva to preserve "thousands" of *unrelated* customer files. Since the directories and tables exceeded any preservation duty, their deletion cannot warrant adverse-inference or monetary sanctions.

When the preservation duty activates, a party must preserve only "what it should, or reasonably should know, will likely be requested in reasonably foreseeable litigation." *Scott v. IBM Corp.*, 196 F.R.D. 233, 249 (D.N.J. 2000); *see also Sarmiento v. Montclair State Univ.*, 513 F. Supp. 2d 72, 94 (D.N.J. 2007), *aff'd*, 285 F. App'x 905 (3d Cir. 2008) (spoliation applies only where it was "reasonably foreseeable that the evidence would later be discoverable"). Once the duty attaches, "the scope of information that should be preserved may remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with an action as it is actually filed." Fed. R. Civ. P. 37, 2015 Am., Advisory Comm. Notes. A corporation need not "preserve every shred of paper, every e-mail or electronic document, and every backup tape."

Zubulake v. UBS Warburg, 220 F.R.D. 212, 217 (S.D.N.Y. 2003). "Such a rule would cripple large corporations," which "are almost always involved in litigation." *Id*.

To illustrate, in *McCann v. Kennedy University Hospital*, 2014 WL 282693 (D.N.J. Jan. 24, 2014), *aff'd*, 596 F. App'x 140 (3d Cir. 2014), plaintiff claimed that he fell in defendant Hospital's emergency room, where Hospital personnel neglected his severe pain. *Id*. at *1. Plaintiff then visited a treatment room, where Hospital employees allegedly ignored and humiliated him. *Id*. Plaintiff sent a letter to the Hospital, threatening to sue and complaining about its "discrimination" and "inhumane treatment." *Id*. at *1–2. The Hospital then deleted footage of plaintiff collapsed on the emergency-room floor, and plaintiff sought sanctions. *Id*. at *3. This Court found that the Hospital's receipt of plaintiff's letter triggered its duty to preserve. *Id*. at *6. But in light of the letter, only litigation based on plaintiff's experience in the *treatment room* was reasonably foreseeable; litigation based on plaintiff's injury in the *emergency room* was not. *Id*. ("[T]he focus of plaintiff's litigation threat was directed to his medical treatment or lack thereof, not what happened in the emergency room lobby."). Although the Hospital's duty had arisen, it did not extend to the emergency-room footage, precluding spoliation. *Id*.; *see also Easterwood v. Carnival Corp.*, 2020 WL 6781742, at *1, 6–7 (S.D. Fla. Nov. 18, 2020) (denying sanctions where cruise-ship operator was bound to preserve only footage of plaintiff's fall, and not footage of another passenger's fall an hour earlier on the same ship).

Just as the *McCann* defendant's preservation duty pertained only to plaintiff's treatment-room experience, any duty purportedly binding Veeva extended only to the Genentech incident. The Genentech incident was isolated and discrete, affecting only 1,350 addresses that Veeva

received from Genentech.[68] Veeva *preserved* the Genentech extract that formed the basis of the incident, foreclosing any "spoliation" or sanctions.[69] By contrast, nearly all of the directories and tables at issue were unconnected to the Genentech incident. They contained data sent to Veeva from *other*, *unaffected* customers. The NAS directories contained data sent to Veeva by [redacted] and others.[70] The HDM tables contained data sent to Veeva by customers such as [redacted].[71] Even if the Genentech incident triggered Veeva's duty to preserve, the Special Master erred in extending that duty to *unrelated* files.

III. Error No. 3: Veeva did not "intend to deprive" IQVIA of evidence.

The Special Master wrongly determined that Veeva "intended to deprive" IQVIA of (1) NAS directories and HDM tables, (2) EUStage, and (3) James Kahan's emails. Dkt. 349 at 75, 81, 88. A "finding of bad faith is pivotal to a spoliation determination." *Bull v. United Parcel Serv.*, 665 F.3d 68, 79 (3d Cir. 2012). The Court may impose adverse-inference sanctions "only" after "finding that the [accused] party acted with the intent to deprive another party of the information's use in litigation." Fed. R. Civ. P. 37(e)(2). "No unfavorable inference arises when the circumstances indicate that the document or article in question has been lost or accidentally destroyed, or where the failure to produce it is otherwise properly accounted for." *Brewer v. Quaker State Oil Ref. Corp.*, 72 F.3d 326, 334 (3d Cir. 1995). "In other words, there must be a finding that spoliation was intentional *and* that there was fraud and a desire to suppress the truth before the Court will make a finding of spoliation." *Bensel v. Allied Pilots Ass'n*, 263 F.R.D. 150,

[68] Ex. 39 at 825–26 (incident implicated [redacted] While the incident also affected a handful of extracts that from other customers, Genentech's was the only one that contained IQVIA data. *Id*. at 834.
[69] *See* Ex. 44.
[70] *Compare* Ex. 39 at 833–34 (scope of incident), *with* Ex. 52 (NAS directories cited by IQVIA).
[71] *Compare* Ex. 39 at 833–34 (scope of incident), *with* Ex. 53 (HDM tables cited by IQVIA).

152 (D.N.J. 2009). Rule 37(e) "rejects cases … that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence." 2015 Am., Advisory Comm. Notes.

An adverse inference is appropriate "*only* when the spoliation or destruction [of evidence] was intentional, *and* indicates fraud and a desire to suppress the truth, and it does *not* arise where the destruction was a matter of routine with no fraudulent intent." *Brewer*, 72 F.3d at 334; *see also GN Netcom v. Plantronics*, 930 F.3d 76, 83 (3d Cir. 2019) (sanctions warranted only where nonmovant "*intended* to impair the ability of a litigant to put on a case"). The "intent to deprive" is absent where materials are deleted for "reasons unrelated to the lawsuit." *Brewer*, 72 F.3d at 334. The party seeking sanctions bears the "burden to prove [the nonmovant's] bad faith conduct," and "there are strong reasons favoring a presumption of inadvertence" rather than "intentional misrepresentation." *Bull*, 665 F.3d at 76–77. "[W]here there is no showing that the evidence was destroyed in order to prevent it from being used by the adverse party, a spoliation instruction is improper." *United States v. Nelson*, 481 F. App'x 40, 42 (3d Cir. 2012).

IQVIA must show not only that Veeva destroyed evidence it was bound to preserve, but also that Veeva did so fraudulently and in bad faith, intending to subvert this litigation. The Special Master erred in concluding that IQVIA met that stratospheric burden.

A. Veeva did not "intend to deprive" IQVIA of NAS directories and HDM tables.

The Special Master erroneously found that Veeva deleted customer data contained in NAS directories and HDM tables with "intent to deprive." Dkt. 349 at 75. Veeva's productions and preservation prove otherwise. Production of "substantial" discovery undermines bad faith. *Applied Telematics, Inc. v. Sprint Commc'ns Co.*, 1996 WL 33405972, at *3 (E.D. Pa. Sept. 17, 1996) (no intentional spoliation where "defendant produced over 800 routing plans" and "devoted substantial resources to its [discovery] responses"). Veeva's productions are beyond "substantial." IQVIA

claims to be interested in customer-data files sent to Veeva so IQVIA can assess whether those files contain traces of IQVIA data, and whether Veeva incorporated those traces into OpenData. As for OpenData, Veeva migrated the OpenData dataset from HDM to Veeva Network in September 2016. Veeva produced full working copies of OpenData and Veeva Network, complete with historical-change logs. Those productions contain all OpenData records that were stored in HDM. As for customer-data files, Veeva preserves those files it receives from (and returns to) its active customers. That includes all Genentech data, to which [redacted].[72] Veeva can produce that data as soon as IQVIA obtains Genentech's consent. IQVIA has not attempted to do so, preferring to litigate spoliation rather than the merits of its own claims. Veeva's vast productions and preservation defeat any semblance of bad faith.

Veeva's sweeping efforts aside, the deletion of documents—even under a duty to preserve—is not sanctionable where it is "susceptible of an innocent explanation." *Scott v. IBM Corp.*, 196 F.R.D. 233, 248 (D.N.J. 2000). Deleting materials pursuant to "ordinary practice" is one such innocent explanation. *See Tabon v. Univ. of Pennsylvania Health Sys.*, 2012 WL 2953216, at *4 (E.D. Pa. 2014). That is what Veeva did. Veeva loaded customer data stored in NAS onto HDM to perform services for customers. When it completed those services, Veeva deleted the files per contractual obligations to customers and its own standard operating procedures.[73] When Veeva obtains authorization to access customer data, that authorization is limited to a particular purpose, such as performing data services for a customer. Once Veeva

[72] Ex. 44.
[73] Ex. 54 at 248:21–249:10; *see also* Ex. 55 at 249 (§ 6) [redacted]

fulfills that purpose, Veeva deletes the data.[74] Such deletion is standard and appropriate—that's why [redacted].[75] IQVIA cannot have it both ways: had Veeva preserved the data, IQVIA would have accused Veeva of violating data-retention policies. As Veeva explained, "As part of the cleanup SOP, if a project had ended and you were no longer engaged, you need to remove any old implementation files."[76] Veeva's ordinary-course deletions cannot support sanctions.

B. Veeva did not "intend to deprive" IQVIA of EUStage.

The Special Master erroneously found that Veeva spoliated EUStage. Dkt. 349 at 78. IQVIA falsely claims that Veeva developed its OpenData Europe product by stealing IQVIA data. Veeva built OpenData Europe using the EUMaster instance[77] of Veeva Network.[78] Veeva has produced a full working copy of EUMaster to IQVIA, including all historical changes made to it. For a brief period, Veeva used the EUStage instance of Veeva Network in conjunction with EUMaster to compile OpenData Europe.[79] During that period, Veeva synchronized data between EUStage and EUMaster, performed all data change requests in EUMaster, and stored most customer data in EUMaster.[80] Once the EUStage instance grew superfluous in February 2016, Veeva decommissioned it and the instance lay dormant.[81] In summer 2018, Veeva migrated its

[74] Ex. 33 at 777 [redacted] Ex. 56 (Veeva 30(b)(6) Tr) at 101:1–7 (Veeva deletes data for "no longer active" customer projects, while retaining data "needed for active projects").
[75] Ex. 33. at 777.
[76] Ex. 54 at 248:24–249:3.
[77] Veeva Network is divided into "instances"—distinct software environments within Network.
[78] Ex. 56 at 168:17, 166:14–15.
[79] Ex. 57 at 093 (EUStage created in February 2015); Ex. 58 at 918 (EUStage decommissioned in February 2016).
[80] Ex. 59 at 74:18–75:16; Ex. 56 at 167:3–23; Ex. 58 at 920.
[81] Ex. 58 at 918; Ex. 59 at 75:12–16.

software to the AWS cloud infrastructure. As part of that transition, Veeva terminated all inactive software instances. Under that even-handed policy, Veeva inadvertently deleted the EUStage instance.[82] Before doing so, Veeva preserved the EUStage data.[83]

1. Veeva deleted the EUStage instance in the ordinary course of business.

Veeva did not "intend to deprive" IQVIA of the EUStage instance. Deletion under a "policy that is even-handedly applied," for "reasons unrelated to the lawsuit," precludes adverse-inference sanctions. *Nelson*, 481 F. App'x at 42. Veeva's 30(b)(6) representative testified that Veeva inadvertently swept EUStage into its general policy of deleting all inactive software instances as it transitioned to AWS.[84] The contemporaneous record confirms that Veeva deleted EUStage alongside other defunct instances unrelated to this lawsuit.[85] IQVIA cited no contrary evidence. Since Veeva's 30(b)(6) testimony went unrebutted, the Special Master had no basis for rejecting it and concluding that Veeva deleted EUStage in bad faith.

At the very least, before deeming Veeva's unrebutted 30(b)(6) testimony non-credible, the Special Master should have held an evidentiary hearing. *Talbird Reeve Sams v. Pinnacle Treatment Ctrs.*, 2021 WL 2010570, at *4 (D.N.J. May 20, 2021) (declining to "question[] the credibility of Mr. Pritchard's declaration" at summary judgment, without a hearing). The court must "be[] able to observe [the declarant's] demeanor and evaluate [his] credibility while on the witness stand." *Fuhs v. McLachlan Drilling Co.*, 2018 WL 5312760, at *14 (W.D. Pa. Oct. 26, 2018) (denying

[82] Ex. 56 at 169:8–22 ("[A]round the time we moved all of our computing infrastructure to Amazon web services," Veeva worked to delete software instances that were either "dead" or "no longer active").
[83] Ex. 56 at 170:19–171:23 ("[R]aw data related to those projects [in EUStage] would exist in the [S3 repository].").
[84] Ex. 56 at 169:8–22; *see also* Ex. 61 ¶¶ 9–10.
[85] Ex. 60.

sanctions and noting case was "distinct from several cases where sanctions have been imposed … where the presiding courts were able to assess the credibility of the alleged spoliators").

The Special Master nonetheless sanctioned Veeva because he found the "timing" of Veeva's EUStage deletion "suspicious" as it shortly followed an interrogatory-response deadline. Dkt. 349 at 81. Deadlines are ubiquitous in litigation—by that reasoning, every accidental deletion mid-litigation would amount to bad faith, defying Rule 37(e). Regardless, "suspicious timing" without more, cannot support an "intent to deprive," particularly where Veeva presented unrebutted evidence of its good faith. No sanctions are warranted.

2. Veeva preserved the EUStage data.

"[B]ecause ESI 'often exists in multiple locations,' spoliation occurs only where the information is truly lost and not recoverable elsewhere." *Bistrian*, 448 F. Supp. 3d at 465. IQVIA requests EUStage so it can examine the customer-data files Veeva loaded onto it, determine whether those files contained IQVIA data, and track whether Veeva incorporated them into OpenData. Although Veeva deleted the EUStage *software instance*, Veeva preserved the EUStage *data*. The Special Master found Veeva's explanation of its EUStage preservation "vague and unconvincing." Dkt. 349 at 80. So Veeva has attached as Exhibit 40 the Declaration of Stanley Wong, which details that preservation. Wong testified, "Veeva preserved all data files that had been processed within the EUStage Network instance in an archive system provided by AWS called the S3 repository. That data remains accessible today. This data includes any data files from third-party sources (e.g., Veeva customers) that may have been processed in the EUStage Network instance before being promoted to the EUMaster Network instance."[86] Since Veeva deleted the EUStage software instance, "certain labels assigned to a data file by Veeva's OpenData Europe

[86] Ex. 40 ¶ 11.

team no longer exist."[87] Nonetheless, "all data files processed in the EUStage Network instance remain preserved in their original state in Veeva's S3 repository."[88]

IQVIA knows that. Veeva told it as much during its 30(b)(6) deposition, three months before IQVIA sought sanctions. Veeva testified that the EUStage files "were archived to something called S-3…. So that archive, that still exists, and that includes the raw data" comprising EUStage, which remains accessible.[89] Veeva disclosed its preservation to IQVIA with the expectation that IQVIA would pursue the data. IQVIA never did so. This Court has unerringly held that "sanctions are a last resort." *Neal v. Asta Funding*, 2014 WL 131770, at *7 (D.N.J. Jan. 6, 2014); *accord Arbitron v. Longport Media*, 2013 WL 12155420, at *2 (D.N.J. Dec. 19, 2013). IQVIA violated that principle by moving for sanctions before requesting the EUStage data. The Special Master violated that principle by imposing sanctions before ordering Veeva to produce the data. Veeva's preservation of the EUStage data—the substance in which IQVIA claims to be interested—forecloses adverse-inference and monetary sanctions.

C. Veeva did not "intend to deprive" IQVIA of James Kahan's emails.

The Special Master wrongly held that Veeva spoliated James Kahan's January 2014–May 2015 emails. Kahan's emails were deleted pre-litigation, before Veeva was bound to preserve them, precluding any sanctions.[90] Moreover, the emails were not deleted with "intent to deprive." Unrebutted evidence proves that Kahan's January 2014–May 2015 emails were deleted to comply with a system-wide per-user email storage limit.[91] Kahan testified that, between January 2014 and May 2015, "there were storage limits per account on e-mails. And as somebody who received a

[87] *Id*. ¶ 12.
[88] *Id*.
[89] Ex. 56 at 169:23–170:18, 171:22–23.
[90] *Id*. at 67:7–21 (any deletions of Kahan's emails occurred pre-litigation).
[91] Ex. 21 at 165:3–16.

large number of e-mails with very large attachments I would reach that limit on a somewhat regular basis."[92] Kahan's uncontroverted testimony disproves "fraud" and "bad faith."

Veeva's 30(b)(6) representative confirmed that several Veeva employees faced similar issues before Veeva removed the storage limits in late 2016.[93] Veeva "offered credible reasons for the destruction of the records" including "storage accommodation," and IQVIA "offered no evidence to rebut that explanation," foreclosing sanctions. *Kitsap*, 314 F.3d at 1001; *see also Peterson v. Seagate US LLC*, 2011 WL 861488, at *3–4 (D. Minn. Jan. 27, 2011) (denying sanctions where nonmovant deleted files "when server storage limits [were] reached" because deletions were "not a result of a concerted effort to suppress evidence"). As with EUStage, the Special Master should not have discredited unrebutted testimony (particularly without an evidentiary hearing).

The Special Master further erred in holding that Veeva acted with "intent to deprive" because Kahan's emails were deleted manually rather than automatically. Dkt. 349 at 88. The "intent to deprive" inquiry hinges not on whether deletion was manual or automatic, but instead on whether deletion stemmed from bad faith. *Brewer*, 72 F.3d at 334. Veeva's uncontroverted evidence proves that Kahan's emails were deleted for "reasons unrelated to the lawsuit," refuting Veeva's "intent to deprive." *See Nelson*, 481 F. App'x at 42.

Further debunking "bad faith," Veeva produced 6,800 of Kahan's January 2014–May 2015 emails from other custodians' files, along with 65,000 of Kahan's emails from outside that period. *See Gaina v. Northridge Hosp.*, 2018 WL 6258895, at *5 (C.D. Cal. Nov. 21, 2018) (no intentional spoliation of text messages where party "made voluminous production of some text messages").

[92] *Id*.
[93] Ex. 56 at 188:20–195:20.

IQVIA's baseless conjecture that Kahan's unproduced emails contained relevant evidence cannot support any sanctions. *GN Netcom*, 930 F.3d at 83 (moving party must show "plausible, concrete suggestions as to what [the lost] evidence might have been"); *Fuhs v. McLachlan Drilling*, 2018 WL 5312760, at *15 (W.D. Pa. Oct. 26, 2018) ("Instead, they have offered conjecture as to what they believe may have been on the devices but that is not enough to justify the imposition of sanctions."); *ML Healthcare Servs. v. Publix*, 881 F.3d 1293, 1309 (11th Cir. 2018) ("Failure to preserve such speculative evidence does not raise the specter of bad faith in the same way that a failure to preserve evidence of a specific, crucial event in a case might.").

D. Veeva's extraordinary preservation efforts disprove its "bad faith."

In amending Rule 37(e), the Advisory Committee urged courts to consider the entirety of the nonmovant's preservation measures before issuing sanctions: "Due to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible.... This rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection." 2015 Am., Advisory Comm. Notes; *see also Applied Telematics, Inc. v. Sprint Commc'ns Co.*, 1996 WL 33405972, at *3 (E.D. Pa. Sept. 17, 1996) (no intentional spoliation where "defendant produced over 800 routing plans" and "devoted substantial resources to its [discovery] responses"); *Martin v. Wetzel*, 2020 WL 6948982, at *3 (W.D. Pa. Nov. 25, 2020) (denying sanctions although "spoliation did occur" where court found "no history of dilatoriness").

A testament to its good faith, Veeva's preservation campaign exceeded the call of duty. Once IQVIA sued, Veeva promptly deployed outside counsel to interview and convey in-person litigation-hold instructions to key individuals.[94] Veeva activated Google Vault to retain emails and

[94] Ex. 56 at 53:9–19; Ex. 20 ¶ 24.

chats, disabling deletion for every current and former employee throughout the global Veeva organization (more than 3,000 people).[95] Veeva instructed its IT department to bar deletions from salesforce.com, Egnyte, Confluence, Zendesk, JIRA, and key Veeva Vault instances.[96]

Veeva did not stop there. It granted its direct competitor IQVIA access to full working copies of the US and EU software instances and databases used to develop Veeva's data products, including historical-change logs. Veeva also produced nearly a terabyte of software log files for Network and OpenData, and a terabyte of HDM information containing Veeva data. Despite the occasional blip inevitable in any complex litigation, Veeva has devoted Sisyphean efforts to its discovery obligations. The Special Master's imposition of adverse-inference and monetary sanctions based on IQVIA's misapplied standards and miscited evidence was error.

III. Fees and costs are not warranted as Veeva did not commit "fraud."

Finally, the Special Master awarded IQVIA costs and fees based on IQVIA's "Fraud Motion."[97] IQVIA claimed Veeva's JIRA-ticket production proved Veeva misrepresented that it lacked information detailing the precise deletion dates of customer-data extracts. IQVIA cannot prove any misrepresentation. Veeva truthfully told IQVIA that it has no "metadata or software logs" containing such information. Dkt. 317 at 17. The JIRA tickets do not demonstrate otherwise. While IQVIA claims Veeva concealed the JIRA tickets until the close of discovery, Veeva had already produced materially identical information.[98] No fraud occurred.

CONCLUSION

The Court should deny IQVIA's sanctions motion in full.

---

[95] Ex. 20 ¶ 28.
[96] *Id.* ¶ 25.
[97] Ex. 47 at 46–47; Ex. 62.
[98] Ex. 61 at 16–17.

Dated: June 4, 2021

Respectfully submitted,

/s/ Joseph A. Hayden, Jr.

Joseph A. Hayden, Jr.
David N. Cinotti
PASHMAN STEIN WALDER HAYDEN, P.C.
Court Plaza South
21 Main Street, Suite 200
Hackensack, NJ 07601
Tel: (201) 488-8200
jhayden@pashmanstein.com
dcinotti@pashmanstein.com

James T. Southwick (*pro hac vice*)
Ryan Caughey (*pro hac vice*)
Michael Brightman (*pro hac vice*)
Robert Travis Korman (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1000 Louisiana, Suite 5100
Houston, TX 77002
Tel: (713) 651-9366
jsouthwick@susmangodfrey.com
rcaushey@susmangodfrey.com
mbrightman@susmangodfrey.com
tkorman@susmangodfrey.com

Michael Gervais (*pro hac vice*)
SUSMAN GODFREY, L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel: (310) 789-3100
mgervais@susmangodfrey.com

Jenna G. Farleigh (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, WA 98101
Tel: (206) 505-3826
jfarleigh@susmangodfrey.com

Steven F. Benz (*pro hac vice*)
Kylie C. Kim (*pro hac vice*)
Christopher C. Goodnow (*pro hac vice*)
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W. Suite 400
Washington, D.C. 20036
Tel: (202) 326-7900
sbenz@kellogghansen.com
kkim@kellogghansen.com
dseverson@kellogghansen.com
csarma@kellogghansen.com
cgoodnow@kellogghansen.com

Charles T. Graves (*pro hac vice*)
Amit Gressel (*pro hac vice*)
WILSON SONSINI GOODRICH & ROSATI PC
One Market Plaza, Spear Tower
Suite 3300
San Francisco, CA 94105
tgraves@wsgr.com
agressel@wsgr.com

Joel C. Boehm (*pro hac vice*)
WILSON SONSINI GOODRICH & ROSATI PC
900 South Capital of Texas Highway
Las Cimas IV, Fifth Floor
Austin, TX 78746
Tel: (512) 338-5418
jboehm@wsgr.com

Counsel for Defendant/Counterclaim-Plaintiff Veeva Systems Inc.